About PKCS#7 SignedData

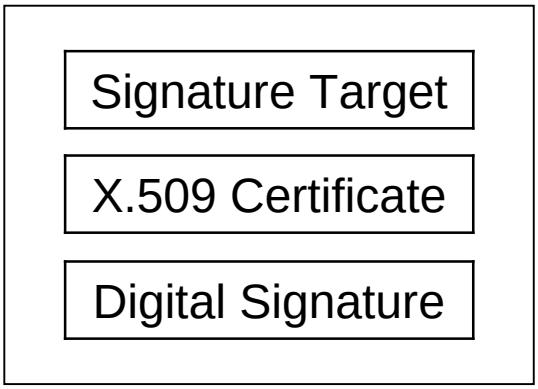
PKCS#7 SignedData has the following ASN.1 syntax.

```
SignedData ::= SEQUENCE {

    version           INTEGER {sdVer1(1), sdVer2(2)} (sdVer1 | sdVer2),

    digestAlgorithms  DigestAlgorithmIdentifiers,

    contentInfo       ContentInfo,

    certificates CHOICE {
        certSet           [0] IMPLICIT ExtendedCertificatesAndCertificates,
        certSequence  [2] IMPLICIT Certificates
    } OPTIONAL,

    crls CHOICE {
        crlSet            [1] IMPLICIT CertificateRevocationLists,
        crlSequence   [3] IMPLICIT CRLSequence
    } OPTIONAL,

    signerInfos     SignerInfos

}



SignerInfos ::= CHOICE {
    siSet             SET OF SignerInfo,
    siSequence  SEQUENCE OF SignerInfo
}
```

```
SignerInfo ::= SEQUENCE {

   version                 INTEGER {siVer1(1), siVer2(2)} (siVer1 | siVer2),

   issuerAndSerialNumber     IssuerAndSerialNumber,

   digestAlgorithm           DigestAlgorithmIdentifier,

   authenticatedAttributes CHOICE {
      aaSet              [0] IMPLICIT SET OF Attribute {{Authenticated}},
      aaSequence         [2] EXPLICIT SEQUENCE OF Attribute {{Authenticated}}
   } OPTIONAL,

   digestEncryptionAlgorithm  DigestEncryptionAlgorithmIdentifier,

   encryptedDigest           EncryptedDigest,

   unauthenticatedAttributes CHOICE {
      uaSet              [1] IMPLICIT SET OF Attribute {{Unauthenticated}},
      uaSequence         [3] IMPLICIT SEQUENCE OF Attribute {{Unauthenticated}}
   } OPTIONAL

}
```

<table>
<tr><td rowspan="6">SignedData</td><td>version</td></tr>
<tr><td>digestAlgorithms</td></tr>
<tr><td>contentInfo</td></tr>
<tr><td>certificates</td></tr>
<tr><td>crls</td></tr>
<tr><td>
<table>
<tr><td rowspan="6">SignerInfo</td><td>version</td></tr>
<tr><td>issuerAndSerialNumber</td></tr>
<tr><td>digestAlgorithm</td></tr>
<tr><td>authenticatedAttributes</td></tr>
<tr><td>digestEncryptionAlgorithm</td></tr>
<tr><td>encryptedDigest</td></tr>
</table>
</td></tr>
</table>

It becomes such a thing as a simple figure.



To make things easier, it means something like this.

Signature target is able to been included or not in PKCS#7 SignedData.

Similarly, X.509 certificates that contain a public key to use for verification are able to included or not.

Verification can be done with only one PKCS#7 SignedData if the PKCS#7 SignedData contains the signature target and X.509 public key certificates containing public key used for verification.

If it is not included, you need to specify it when performing validation.

PKCS#7 SignedData may contain multiple X.509 certificates and multiple signatures (multiple SignerInfo).

Multiple X.509 certificates are used, for example, if all of the X.509 certificates have been bundled for certificate chain validation.

Multiple signatures are used, for example, when signatures are being signed by multiple people.